Mr Charles Kane Committees 8

UNITED STATES INTELLIGENCE BOARD
SECURITY COMMITTEE

SECOM-D-56
2 April 1975

MEMORANDUM FOR: Security Committee Members

SUBJECT : Guidelines for Sanitizing Certain Documents Provided Select Committees

1. The attached draft guidelines on sanitization were prepared on an expedite basis for the Chairman, USIB Ad Hoc Coordinating Group on Congressional Reviews.

2. It was disseminated by the Chairman to Principals of the Ad Hoc Group and at a meeting of the Group on 2 April 1975 it was decided that the Principals would review the draft in coordination with their Security Committee representatives and recommended changes would be furnished to the members of the Security Committee. Following this it was requested that the Security Committee meet to consider the draft and suggested changes and prepare revised guidelines for submission to the Ad Hoc Group at an early date.

3. It is requested that the Security Committee members review the attached draft and be prepared to meet on the subject matter early during the week of 7 April.

4. It would be helpful if members called to the attention of the Chairman or the Executive Secretary of the Security Committee any major changes desired in the draft.

[redacted]

25X1A

Chairman

Attachment

83 51552

DRAFT
28 March 1975

GUIDELINES FOR SANITIZING CERTAIN DOCUMENTS PROVIDED SELECT COMMITTEES

1. The Director of Central Intelligence has recently discussed with Senator Church the need for special consideration and treatment by the Select Committee of certain sensitive aspects of intelligence activities and the Senator has expressed his recognition of this need. Included in such matters are the identities of sensitive sources, the material provided to the United States by cooperating foreign intelligence services, the details of technical devices and systems and of operational methods, the identities of certain employees whose safety could be jeopardized if revealed, the identities of American citizens and organizations who have cooperated with US intelligence and some additional materials the public disclosure of which would create serious foreign policy or national security problems. Such material should be protected not only from exposure but indeed the risk of exposure. Further, recognition should be given to the need to protect certain other information which, if improperly disclosed, might impair the privacy rights of individuals.

2. One form of this special consideration may include use of sanitization procedures to avoid the risk of exposing such matters and at the same time satisfy the Select Committee's need for a full understanding of the community's activities.

3. What May Be Sanitized

While it is not possible to anticipate all requirements which may be levied by the Committees for documenting material and not possible to determine specifically what material should be excised from these documents, the following illustrations are offered in certain likely categories. The criteria in all cases should meet the test mentioned above.

4. Collection of Intelligence

(a) The Committee will probably address the matter of how intelligence activities or methods have or may impinge upon individual rights. Documents supporting responses may be sanitized by removal of identities of sensitive agents and informants, covert personnel, and contractual cover arrangements. A descriptive phrase may be substituted, i.e., a foreign journalist, a political official in the opposition party. No sanitization should be used in connection with

Approved For Release 2002/05/01 : CIA-RDP83B00823R000700040013-3

names of individuals whose employment or former employment by, or association with a department or agency, does not remain secret or for individuals whose present or future activities on behalf of the department or agency do not require that previous cover arrangements remain secret.

(b) Some information may be required with respect to technical intelligence systems including cryptologic and communications activities and reconnaissance capabilities. Almost all of such material is currently handled in compartmentation control channels under various codewords or nicknames. No security threat is perceived by release of these codenames or nicknames in documents. Details of the technical systems involved, contractual arrangements, funding and/or names of companies or consultants whose participation was obtained under agreement of continued secrecy may be excised from documents. Any question on release of codeword material should be referred to the Program Manager who in turn may consult with the Director of Central Intelligence to ensure a consistent approach in the community's sanitization procedure. While documentary samples of intelligence obtained by technical means may be used in support of verbal testimony, no raw product should be provided the Committees

for retention. If absolutely required by the Committees, sanitization of such raw product should be conducted to mask the degree of technical capabilities.

5. Intelligence Estimates

Finished intelligence reports of departments and agencies and estimates do not usually contain source identifications and will not normally require sanitization. However, departments and agencies should review such publications to ensure deletion of source identities.

6. Administration

Information concerning the internal administration arrangements of intelligence agencies may be requested. This may include staffing chartswith occupants identified. / Identities of personnel formerly not under cover and now functioning in a cover assignment should be deleted as well as those who may in the future be considered for a covert assignment.

7. General

The following categories of information or specific examples may arise in any number of circumstances in documentation requested by the Select Committees. In all cases, serious consideration should be given by the department or agency concerned to the necessity of

deletion or sanitization of this type of information, prior to providing the document.

(a) Agent or informant names or operational information revealing them.

(b) Details which would reveal the effectiveness of sensitive methods and techniques (1) employed overseas in human source collection, (2) employed for the physical security protection of the department's or agency's personnel or physical environment.

(c) The numbers, locations, times and other indications of recruitment or emplacement of personnel within targetted foreign organizations.

(d) The success or failure of recruitment attempts in any given targetted foreign organization.

(e) Names of particular employees whose physical safety or future career might be placed in jeopardy by exposure.

(f) Foreign or US sources, official or otherwise who agreed to cooperate under terms of explicit or implied confidentiality, who would be embarrassed or endangered by disclosure of their role.

(g) Identifying information on intelligence services in friendly and neutral countries.

(h) Identifying collaborative operations between the United States intelligence agencies and other foreign intelligence liaison services against targets within the country extending the collaborations or within a jointly targetted third country.

(i) Identifying collaboration with foreign governments in signals intelligence collection, particularly for arrangements which, if revealed, would be politically embarrassing in the countries involved.

(j) Identification of technical intelligence operations of high technical vulnerability and extremely high political sensitivity.

(k) Specific identification of foreign technical collection installations involving high political sensitivity in the host country.

(l) Details or disclosure of monetary arrangements with US and foreign banks, investment houses, etc., in support of foreign intelligence operations.

(m) Specific information on special relationships with private firms established with the approval of top corporate officials. This includes names of firms or industrial associations that collaborate in a special manner such as providing cover for foreign intelligence operations.

(n) Names of firms collaborating with US intelligence agencies in collection and assessment programs (especially those having large foreign clienteles).

(o) Proprietary information relating to contractors or furnished in confidence.

8. What Should Not Be Sanitized

There are general categories of intelligence activities which have already been placed in the public domain by the mass news media or authors with background experience in intelligence departments or agencies of the community. Names, places, dates and events which have been so revealed should not be excised if contained in requested documents.

There is an increasing body of information which has been released under the Freedom of Information Act. No further sanitization of this material should be conducted unless it relates to an individual's rights to privacy.

9. Techniques of Sanitization

Sanitization of intelligence material is usually considered the act of physical removal of the identity of a person, place or thing from written communication with or without regard for the residual

content. Use of a substitution device, either pseudonym or ident is an example of sanitization which permits intelligent continuity of the material without revealing the true identity. Sanitization does not extend to the use of false or misleading substitute material in this context.

The integrity of official records must be maintained. The following sanitization techniques apply only to copies of records.

(a) Physical Sanitization - Names may be cut out and the residual material xeroxed and submitted to Committees. Names may be masked with correction tape and then xeroxed. The xerox copy may be submitted to the Committees.

(b) Names may be deleted and replaced with "IDEN." The deleted material is provided on a separate IDEN list which contains names or descriptive phrases substituted for deletions.

(c) The material can be retyped or reprinted with substitute phrases or substitute descriptions which do not reveal the sensitive material.

(d) Entire pages can be removed from some documents and replaced with a blank page carrying only reference information

as to the location of the sensitive material within the contributing department or agency. This technique may be employed when physical sanitization or excision of material results in unintelligible gibberish as residue.

(e) Within a category of inquiry, it may be desirable to extract a complete document from requested material when the request is broad and all inclusive within its field. The existence of such a document should be made known to the Committees but retained by the agency or department for review under escort of a representative of the department or agency.

10. Management of Sanitization

The original record and a copy of the sanitized version provided should be readily available in all cases. Materials developed within an agency or department in response to requests should be reviewed at an appropriate level for completeness, responsiveness and accuracy. In the case of documents or materials of a community nature, the release should be done in coordination with the departments or agencies and/or the Program Manager concerned and any sanitization should be agreed upon during coordination.

This proposed use of sanitization as a special arrangement to protect selected issues contained in material provided to Select Committees by one agency may prove to be a futile exercise if not practiced in common by all participating departments and agencies. It is essential to the proposal that departments and agencies attempt to employ the same criteria for sanitization and coordinate as required. This paper can serve only as general guidelines on sanitization.